ITEA Journal 2009; 30: 300–308

Development of an Ontology-Based Tool to Support the Test and Evaluation Process for Rapid Acquisition of IED Detection Capabilities

Paul M. Franken, A. Jay Harrison, J. Jerome Holton, Ph.D., D. Luke Macfarlan, and Zenovy S. Wowczuk, Ph.D.
ARES Systems Group, LLC, Vicksburg, Mississippi
N. Clark Capshaw, Ph.D.
U.S. Army Evaluation Center, Alexandria, Virginia
Randall W. Williams
U.S. Army Engineer Research and Development Center, Vicksburg, Mississippi
David J. Russomanno, Ph.D.
Center for Advanced Sensors,
Department of Electrical and Computer Engineering, University of Memphis, Memphis, Tennessee

An adaptable adversary with a 30-day innovation cycle has driven the demand for a rapid acquisition process that compresses the current acquisition cycle. We describe the development of a tool for the Test and Evaluation (T&E) community to enable consistent and objective application of threat intelligence to a subset of the rapid acquisition enterprise: Counter-Improvised Explosive Device (C-IED) sensor testing. Currently there is no single standard common to all T&E entities regarding development and application of threat phenomena to C-IED sensor testing, which results in T&E products that do not readily support the direct comparison of system performance. A tool is needed to engage the T&E community to define and automate best practices to enable a consistent application of threat phenomena. The Joint IED Defeat Test Board is developing a Common IED Exploitation Target Set (CIEDETS), an ontology-based decision support tool that provides consistent, repeatable application of operationally realistic threat information to C-IED sensor T&E efforts. The goal is to implement a documented methodology for the development of surrogate threat "observables" applicable to the full spectrum of C-IED sensor T&E scenarios. This article overviews the CIEDETS technology and describes how CIEDETS could be utilized for individual system evaluation and to augment the system-of-systems evaluation of an integrated aerial Intelligence, Surveillance, and Reconnaissance (ISR) Task Force.

Key words: Counter-IED sensor testing and evaluation; observables; ontology-based decision support architecture; rapid acquisition; repeatable application of threat signatures.

The U.S. Department of Defense Counter-Improvised Explosive Device (C-IED) community has compiled an extensive inventory of data on IED threat signatures and tactics. Currently this inventory consists of various independent data sets, which are organized according to widely disparate standards and maintained by a diverse set of user groups. The Joint IED Defeat (JIEDD) Test and Evaluation (T&E) community uses available threat

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Development of an Ontology-Based Tool to Support the Test and Evaluation Process for Rapid Acquisition of IED Detection Capabilities	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Evaluation Center,4501 Ford Ave,Alexandria,VA,22302-1458**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**9**	

information to produce threat representations against which C-IED sensor technology performance can be validated. The availability, accuracy, and standardization of threat information are critical to the effectiveness of the overall C-IED enterprise.

The T&E community's ability to harvest IED-related threat information in a consistent and repeatable manner is limited by the absence of a formal model that explicitly correlates IED observables and associated signature data with C-IED sensor technologies and associated mission profiles. A standardized approach offers the following advantages:

- minimization of duplicative testing,
- consistent and repeatable application of threat signature data for the development of event-specific Threat Test Support Packages (TTSP),
- more timely and efficient utilization of unstructured threat information for system T&E, and
- detailed documentation of the test objectives and constraints used in determining the test setup.

The Common IED Exploitation Target Set (CIEDETS) is an ontology-based decision support tool that provides a structured framework for defining T&E objectives and correlating these objectives to an optimum set of threat observables that can be used to exercise the performance of C-IED technologies in operationally realistic contexts. The current instantiation of CIEDETS focuses on the "detect" mission thread of the overall C-IED enterprise. CIEDETS is initially planned to be a component of the Army Test and Evaluation Command evaluation of individual electro-optical, infrared, and radar-based systems and ultimately to assist in an integrated aerial Intelligence, Surveillance, and Reconnaissance (ISR) Task Force system-of-systems evaluation.[1]

CIEDETS and the role of the Joint IED Defeat Test Board (JTB)

The JTB synchronizes JIEDD T&E events within the Department of Defense and assists the Services and Joint Commands to maximize utility and decrease redundancy in testing of JIEDD initiatives. To this end, the JTB is the lead agency for coordinating JIEDD T&E events to optimize potential opportunities for collaboration, avoid test duplication, reduce redundancy of test resources, minimize the time required to provide solutions to the field, and facilitate common test methodologies and data element dictionaries.[2] As part of this mission, the JTB is developing a series of protocols governing T&E of the full range of C-IED capabilities and systems. JTB T&E protocols define specific guidance and community best practices, including quantifiable measures of performance and measures of effectiveness, related to C-IED system T&E as well as data collection and reporting standards.

JTB T&E protocols provide overarching guidance for the conduct of C-IED-related T&E activities. This guidance serves to ensure a level of consistency and repeatability in tests across the JIEDD community that would not otherwise be possible in the absence of a unifying standard. Whereas ultimate responsibility for C-IED test plan development and execution remains with the Service Operational Test Agencies, the JTB, through the implementation and enforcement of T&E protocols, is responsible for collecting and promulgating the C-IED test objectives and reporting standards specified by the operational community and Joint IED Defeat Organization to justify system acquisition and deployment decisions.

CIEDETS is an emerging key component of the JTB protocol development effort. Within this context, CIEDETS functions as the primary decision support system for the definition of threat observables that correspond to different C-IED sensor technologies. As protocols are developed, CIEDETS is employed to record information regarding specific sensor technologies, anticipated mission profiles, deployment platforms, and environmental considerations. From these inputs, CIEDETS generates a corresponding set of observable threat characteristics that a test range should seek to replicate in a test program to exercise a System Under Test (SUT) across a range of desired operational conditions. The CIEDETS output constitutes the basis for the threat definition published in the JTB sensor test protocols.

CIEDETS system design

CIEDETS is the JTB's pilot effort to develop and deploy a standardized approach to integrate and exploit threat information in support of C-IED sensor T&E activities. This project involves implementation of a formal knowledge and data model that integrates IED threat information from multiple sources to derive a set of IED observables. For this application, "observables" are defined as the characteristics of the IED along with the artifacts of IED manufacturing and emplacement that may be directly or indirectly detected in the electro-magnetic spectrum (e.g., size, color, metallic composition, explosive composition, etc.).[3] CIEDETS is designed to correlate the IED observables with user-defined C-IED sensor technologies, deployment platforms, and associated mission profiles in order to define an optimum set of threat characteristics required to test those sensor technologies in specified operational environments. CIEDETS links system performance characteristics to desired mission capabilities (Simmons and Wilcox 2007).

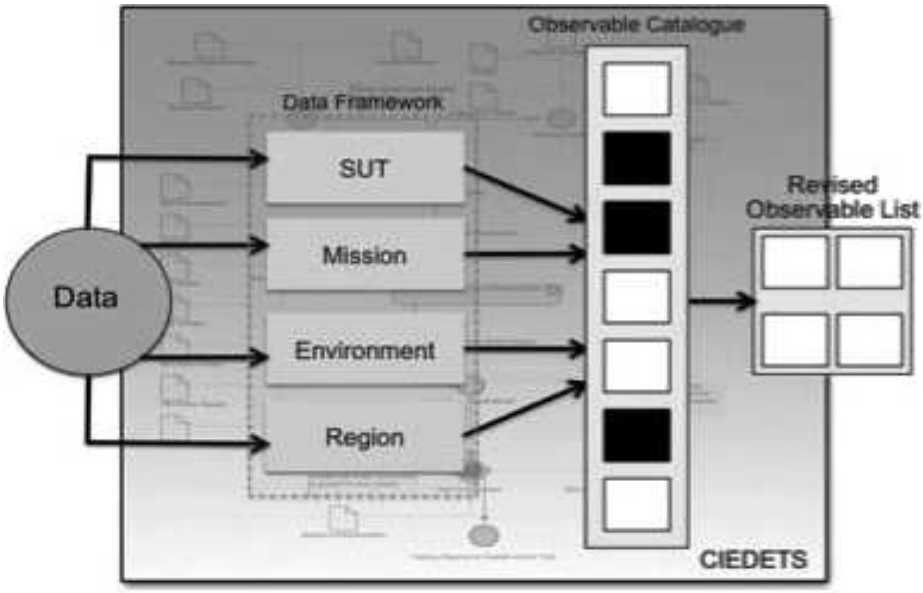

Figure 1. Common improvised explosive device exploitation target set system diagram.

CIEDETS also explicitly defines relationships between existing IED-related threat data sources and key nodes in the IED threat enterprise to include recruiting, training, logistics, supply, and device deployment. The resultant ontology is part of a dynamic decision-support framework that filters and organizes IED threat data based on user-defined instance data consisting of C-IED sensor technology information, deployment platform, and associated mission parameters.

As a T&E planning tool, CIEDETS correlates specific sensor phenomenology, associated mission profiles, platform capabilities, and environmental variables with a comprehensive catalog of threat observables. CIEDETS maps this resulting subset of optimized observables to existing threat signature data sets to enable the JIEDD T&E community to identify and reference technical data relevant to the development of physical IED threat representations.

Figure 1 shows a system diagram of the CIEDETS tool. Within this construct, CIEDETS provides a structured, ontology-based framework to capture key test conditions that characterize four elements: (1) the *SUT*, (2) the operational *Mission*, (3) the deployment *Environment*, and (4) the deployment *Region*. The structured input deck is automatically correlated to the IED threat observables catalog, producing a refined list of observables that are required to exercise the given system relative to the operational mission, environment, and region.

Ontology-based decision support architecture

The development of a standard ontology for missions, platforms, and sensors is not a new concept. Several research and development efforts have been undertaken by the government, private industry, and universities to formulate an ontological structure that could be used to match sensors to specific mission profiles (Gómez et al. 2008). These efforts have focused mainly on developing a highly probable matching of sensors to fulfill a specific mission task based on historical mission data and sensor specifications (Preece et al. 2008). The focus of CIEDETS is to leverage previously designed data models and introduce a capability to simultaneously associate current threat data with individual sensors, integrated systems, C-IED mission profiles, and environmental considerations.

The CIEDETS ontology development has three main concentration areas: (1) establish a robust input relationship architecture to standardize the T&E planning process, (2) create a comprehensive IED threat observable catalog that is driven by current intelligence data from various source providers, and (3) create a semantic tagging association structure and logic engine that matches the input ontology with relevant threat observables. The tagging association structure consists of a correlation function that associates mission-specific input parameters with corresponding threat observable attributes. Threat observable attributes are both qualitative and quantitative and define the basic temporal, spatial, and contextual characteristics of the threat. *Table 1* lists several examples of CIEDETS threat attributes.

The CIEDETS input ontology uses existing conceptual data models (Russomanno, Kothari, and Thomas 2005) developed for mission planning applications to provide a logically consistent framework

Table 1. Common improvised explosive device exploitation target set threat attributes.

Attribute	Description	Units
Changed area	Small change	ft^3
	Medium change	ft^3
	Large change	ft^3
Object size	Small	ft^2
	Medium	ft^2
	Large	ft^2
Linear aberration	Small	ft
	Medium	ft
	Large	ft
Observable speed	Low	ft/s
	Medium	ft/s
	High	ft/s
Radar cross section	Small	ft^2
	Medium	ft^2
	Large	ft^2
Contrast thermal	Low	°F
	Medium	$°F$
	High	$°F$

within which test conditions can be decomposed and recorded (Goodwin and Russomanno 2006; Russomanno, Kothari, and Thomas 2005). The ontology includes a logic-embedded input variable format that relates the SUT, the executable mission type, and the operational environment in a single test profile description. The CIEDETS logic engine correlates the test profile with an integrated IED threat observable catalog to identify a refined set of observables that are most relevant to the input conditions. The fitness of individual observables is determined using a hybrid-rule-based approach, which integrates heuristics with modeling and simulation results. The CIEDETS process enables users to quickly identify the IED threat observables most relevant to the test conditions and capture a pathway description of the test setup.

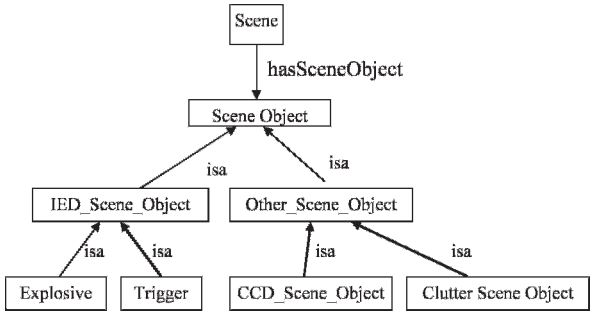

Figure 3. Excerpt of common improvised explosive device exploitation target set observables ontology structure.

CIEDETS enforces data integrity constraints to ensure internal consistency between test input conditions (Thomas and Russomanno 2005). The input conditions are organized into four areas: (1) the SUT, (2) the operational mission profile, (3) the environment, and (4) the region where the system will be deployed. An excerpt of the taxonomic decomposition of the input CIEDETS ontology and the output structure is shown in *Figures 2 and 3*, respectively. The input ontology captures the attributes and relationships among the components that comprise the SUT, including the various sensing modalities and platform, the operational mission, environment, and region. The output CIEDETS ontology captures the attributes and relationships among the entities that comprise the IED observables, including the explosive, the trigger, the camouflage, cover, and concealment, as well as the background clutter objects in the scene. The logic engine processes the rule base to derive implicit associations, such as *can detect* relationships, between the SUT and the observables. Users are alerted to instances where logical inconsistencies between input conditions may exist and they are prompted to adjust the affected inputs appropriately.

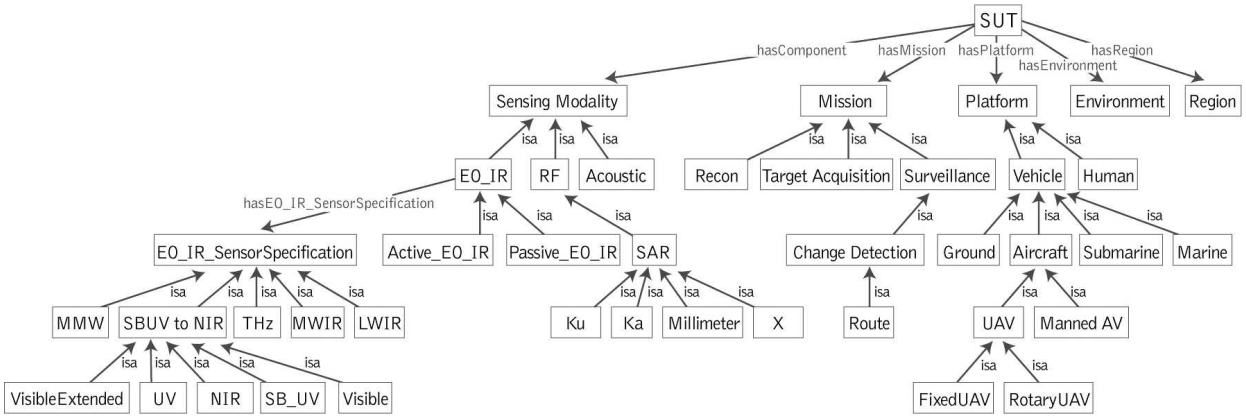

Figure 2. Excerpt of common improvised explosive device exploitation target set input ontology structure.

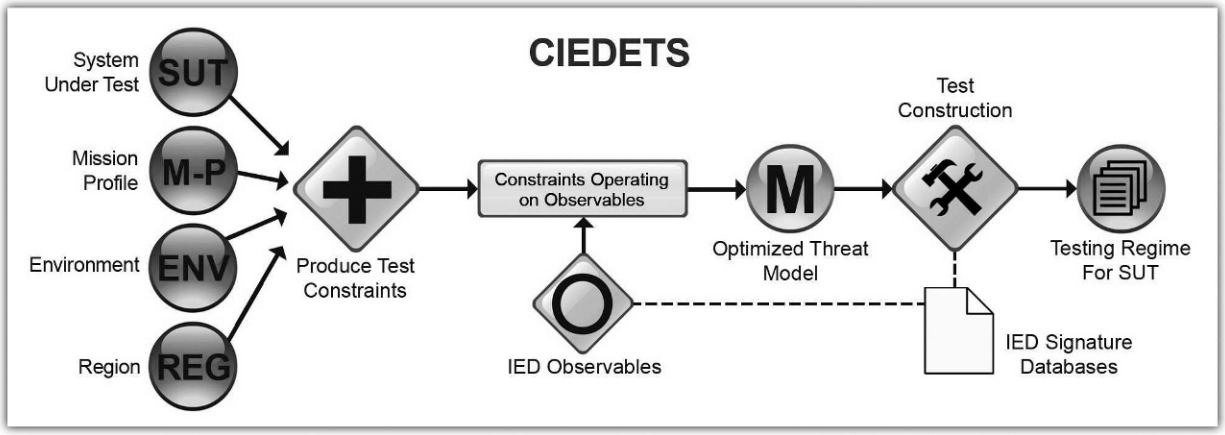

Figure 4. The common improvised explosive device exploitation target set system diagram and contribution to the test and evaluation process.

JIEDD T&E lexicon

To standardize the test and evaluation of developmental sensors for C-IED detection, a common understanding of related terminologies is required. In parallel with the development of the ontology structure mentioned earlier, the CIEDETS system includes a JIEDD T&E lexicon that provides a standard reference for the terminology used in the CIEDETS tool. The multipurpose lexicon serves as both the terminology bridge for standardization throughout the JIEDD T&E community and, through a web-enabled interface, a resource for capturing in-theater reporting and context to update and inform the concepts expressed in the lexicon.

The JIEDD T&E Lexicon employs social networking technology in the form of a wiki engine that enables continuous refinement and updating of IED-related terminology by the operational military and T&E communities. Given that the JIEDD T&E Lexicon is designed to be the authoritative terminology reference for JIED-related T&E activities, an adjudicating body under the JTB reviews the proposed content before the term is permanently updated. The adjudicating body has the ultimate authority on whether to modify the current description or to leave the suggestion on the page as a "note" or "opinion." Terms specified in the CIEDETS ontology are dynamically linked to the JIEDD T&E Lexicon. When a user encounters a term in the ontology, the wiki-based lexicon provides seamless access to the community-approved definition.

CIEDETS T&E support tool

The structured framework of the CIEDETS ontology, the logic-driven CIEDETS engine, and the integrated JIEDD T&E Lexicon collectively provide the T&E community with a standardized resource for defining the optimum set of IED-related threat observables required to comprehensively exercise a given SUT across a range of operational conditions. To further enable commonality in test execution, CIEDETS includes a library of test structures and associated observables for common C-IED-related mission profiles. Additional functionality enables users to save new test profile templates for future reference so that specific test conditions can be replicated in subsequent test events. *Figure 4* provides a system-level view of the CIEDETS application and indicates where CIEDETS fits in the T&E process.

The CIEDETS system output consists of a set of threat observables that are optimized to specific test objectives. The output observables are referenced to a distributed network of IED signature databases that are populated and maintained by organizations throughout the JIEDD community.[4] Within this context, CIEDETS is designed to function as a single point of entry for the T&E community to efficiently exploit heterogeneous IED signature data sets. Threat observables, along with the underlying signature data, are in turn used for the development of physical threat representations or TTSP that can be deployed within the context of a live test event. *Figure 5* is an example of the instantiated CIEDETS output, which was generated by the logic engine, for a specific test scenario.

The development path for CIEDETS includes the introduction of a statistical toolkit that enables users to determine the optimum number of unique data points required to establish a predetermined confidence interval for system performance as a function of test setup and execution constraints. The toolkit can be used to measure the direct correlation between individual observables in order to reduce the total number of unique observables required for deployment within a given test event. The correlation measure is

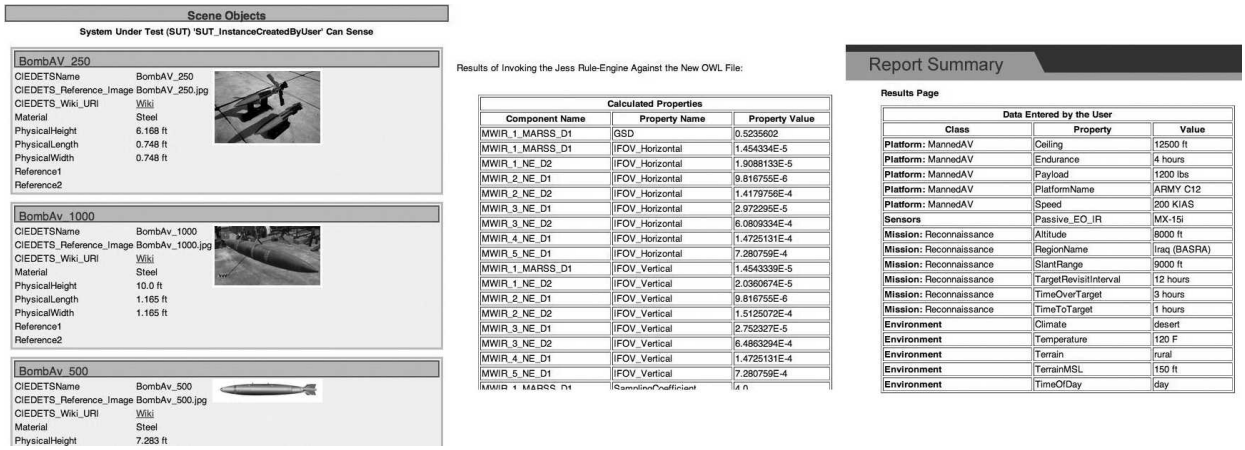

Figure 5. Common improvised explosive device exploitation target set system output.

also useful in determining the relative distribution of observables with respect to the IED detection modes being exercised within the context of a system test.

Once deployed, CIEDETS will be accessible via a Secure Internet Protocol Router network web portal maintained by the JTB. The portal provides a common environment for real-time knowledge sharing between disparate test centers within the C-IED enterprise to enable optimization of limited T&E resources for the rapidly evolving asymmetric threat environment.

Potential use case execution: Aerial ISR Task Force

Phase one of CIEDETS development includes creating a robust structured ontology, fusing the ontology with current threat intelligence, and deploying CIEDETS in a limited capacity to support a specific C-IED-related T&E effort. The initial use case for the CIEDETS tool will focus on electro-optical, infrared, and radar-based systems used to detect and characterize phenomena related to the Terminal Phase of IED deployment. The Terminal Phase of IED deployment refers to enemy activities directly associated with the following:

1. Enemy ingress—movement of personnel or materials associated with the physical emplacement of a device or series of devices,
2. Device deployment—physical emplacement of a device or devices to include enemy reconnaissance and surveillance and prepositioning during device emplacement and/or detonation, and
3. Enemy egress—movement of personnel or materials following the emplacement of a device or series of devices.[5]

Figure 6 depicts an infrared observable associated with the Terminal Phase of IED deployment.

An initial use case for CIEDETS could involve an aerial ISR Task Force system-of-systems evaluation effort. The U.S. Army has deployed an aerial ISR Task Force since 2006 with the mission to conduct operations for the detection and characterization of threats and threat networks. Throughout its initial operational phases, the aerial ISR Task Force has become a key operational component for emerging sensor technologies that have been developed to exploit characteristics of the IED threat, both left and right of "boom."

Early systems deployed as part of the aerial ISR Task Force were subjected to disparate test regimes even in cases where the systems in question were of the same capability. The absence of a formalized threat baseline for system validation resulted in performance expectations that were not consistent with stated individual system capabilities and an inability to directly compare system performance when functioning as a system-of-systems.[6] The CIEDETS development effort was initiated, in part, to address lessons learned from these experiences. As part of further aerial ISR Task Force evaluation efforts, CIEDETS can be used to support TTSP development for individual system T&E in order to validate the efficacy of systems relative to a common benchmark. CIEDETS can also support the continuing and future system-of-systems level evaluation of the aerial ISR Task Force enterprise by assisting in the definition of comprehensive threat profiles that can be used to measure the complementary nature of discrete sensors working in tandem to characterize different aspects of the IED threat.

The CIEDETS objectives for a potential aerial ISR Task Force use case include demonstrating a reduction in the overall time required to develop a threat profile for a given system test by 50 percent, enabling traceability of all TTSP elements to validated threat intelligence, and providing a distributed, network-

Figure 6. Improvised Explosive Device (IED) emplacement activity associated with the Terminal Phase of IED deployment.

addressable environment for sharing threat profile information between test centers.

Future work

Phase two of the CIEDETS effort will address expansion of the ontology structure to include threat-related information and associated technology relationships outside the electro-optical/infrared and radar domains. The objective CIEDETS capability will furnish a single resource for comprehensively correlating IED characteristics with C-IED technologies across the five IED defeat mission threads: predict, detect, prevent, neutralize, and mitigate (Baker and D'Aria 2005). Additional effort will focus on more completely mapping available threat intelligence and associated threat signature databases to the CIEDETS observables to ensure that CIEDETS provides a pathway to underlying data sources relevant to the development of TTSP.

CIEDETS is part of a larger effort being undertaken by the JTB to synchronize the overall JIEDD T&E enterprise. JTB envisions deploying a set of centrally managed, mutually reinforcing applications that will enable different test centers operating independently from one another to leverage a common set of analytical tools and associated databases in the execution of constructive test events. These constructive tests will provide a more robust understanding of the impact of individual technologies on the overall C-IED mission set and support more informed acquisition decision-making. ❑

Paul Franken is a director of Global Security Consulting with ARES Systems Group, located in Alexandria, Virginia. ARES supports the U.S. Army Test and Evaluation Command and other members of the Test, Threat, and Evaluation community. The company provides technical, tactical, and material solutions to federal and commercial clients. He was an active-duty Army Aviator with tactical experience in Stability and Support Operations (SASO) and a veteran of Operation Iraqi Freedom (OIF 1). He holds a Bachelors of Arts in History from Ripon College in Ripon, Wisconsin. E-mail: pfranken@ares-sg.com

Jay Harrison is the managing director of ARES Systems Group. His education includes a bachelor of arts degree in philosophy from the University of Memphis, Memphis, Tennessee; a master of science degree in nuclear Engineering and a MS in aerospace engineering from the University of Florida, Gainesville, Florida; a master of arts degree in national security and strategic studies from the Naval War College, Newport, Rhode Island. He is also a graduate of the Joint Military Intelligence College, Washington, DC. Mr. Harrison led a distinguished career in the Department of Defense Civil Service where he was instrumental in developing current Army policy for the execution and evaluation of Rapid Acquisition Initiatives. During this period, Mr. Harrison achieved the distinction of being awarded multiple Army Greatest Invention awards for his contributions to technology innovation in the public sector. He has 15 years of experience in the direct management, execution, and evaluation of advanced technology programs and is a widely recognized leader in the area of rapid technology incubation for defense and security applications. E-mail: jharrison@ares-sg.com

Dr. J. Jerome Holton is a senior vice president and chief technology officer for ARES Systems Group, located in Alexandria, Virginia. He brings more than 15 years experience in the government and commercial sectors,

providing subject matter expertise on policy, technology, and operational issues for weapons of mass destruction. He has a bachelor of science degree in physics from Mississippi State University in Mississippi State, Mississippi, as well as a master of arts degree and a doctor of philosophy degree in physics, both from Duke University in Durham, North Carolina. Currently, Dr. Holton leads a team of subject matter experts in the development of multidomain intelligence, surveillance, and reconnaissance (ISR), information operations (IO), and force protection systems, architectures, and technology concepts to mitigate the full spectrum of asymmetric threats in the global security environment. E-mail: jholton@ares-sg.com

Luke Macfarlan is a senior research associate at ARES Systems Group. Mr. Macfarlan holds a bachelor of arts degree in history from James Madison University in Harrisonburg, Virginia. At ARES, he supports customers by planning and executing management and technology solutions engagements, specifically through the identification and deployment of multidisciplinary solutions designed to help organizations and governments compete more effectively in the contemporary global security environment. Mr. Macfarlan served in Operation Iraqi Freedom as a SECFOR platoon leader with the Virginia Army National Guard. E-mail: lmacfarlan@ares-sg.com

Dr. Zenovy Wowczuk is a senior research associate at ARES Systems Group. He holds a doctor of philosophy degree in civil engineering, master of science degree in mechanical engineering, and bachelor of science degree in mechanical engineering, all from West Virginia University in Morgantown, West Virginia. He has a diverse background in aircraft system design and development as well as experimental testing of novel systems on-board military airframes. Dr. Wowczuk is well versed in product deployment and commercialization of technology developed from basic and applied research, and has U.S. patents covering add-on sensor/electronic payload systems for military aircraft and several additional patents pending that relate to novel sensor/antenna deployment techniques and methodologies for various airframes. E-mail: zwowczuk@ares-sg.com

Dr. Clark Capshaw is an evaluator with the U.S. Army Test and Evaluation Command, in Alexandria, Virginia, and an online instructor for the University of Phoenix. He has been the evaluator on several aerial ISR systems, including Task Force Observe, Detect, Identify, Neutralize (ODIN). His education includes a master of science degree in aerospace engineering from the University of Dayton, located in Dayton, Ohio, and a doctor of philosophy degree in leadership and policy studies from Vanderbilt University in Nashville, Tennessee. E-mail: Norman.Capshaw@us.army.mil

Randall Williams is a civilian government scientist with the U.S. Army Engineer, Research, and Development Center (ERDC), Vicksburg, Mississippi. He has more than 30 years of technical experience performing RDT&E and training for development of improved Blue-Forces protection suites, future warfare considerations, threat assessments, intelligence restructuring and combat readiness assessment, red teaming, Counter-IED and surface phenomenology, C4ISR, and targeting sensor systems development and defeat of threat-based denial and deception. He has been thrice awarded the Director of Central Intelligence Excellence Award for his efforts in countering threat denial and deception practices and holds a coveted Jasons' Special Service Award. He has a master of science degree in environmental engineering and sciences from the University of Florida in Gainesville, Florida, and a bachelor of science degree in environmental sciences from the University of Southern Mississippi, located in Hattiesburg, Mississippi. E-mail: randall.w.williams@usace.army.mil

Dr. David J. Russomanno is the R. Eugene Smith professor and chair of the Department of Electrical and Computer Engineering at the University of Memphis, Memphis, Tennessee. He received the bachelor of engineering degree in electrical engineering from Auburn University, Auburn, Alabama, in 1986. He received a master of engineering degree in electrical and computer engineering and a doctor of philosophy degree in computer engineering from the University of South Carolina, Columbia in 1989 and 1993, respectively. Dr. Russomanno has also been employed by Pratt and Whitney Aircraft, Intergraph Corporation, and Michelin Tire Corporation. His research interests include intelligent sensors, knowledge representation for the semantic web, data migration and visualization techniques, logic programming applications, and engineering information management systems. E-mail: drussmnn@memphis.edu

Endnotes

[1]"New 'Spies in the Sky' Task Force to Go Operational," *Aviation Today*, May 11, 2007. http://www.avtoday.com/rw/topstories/11325.html (accessed October 6, 2008).

[2]Department of Defense Directive 2000.19E, "Joint Improvised Explosive Device Defeat Organization," February 14, 2006.

[3]"The Joint IED Defeat Test Board Wiki," June 6, 2008. http://10.0.1.50/mediawiki/index.php/(U)_Main_Page (accessed September 29, 2008).

[4]"Target Catalog," September 8, 2008. http://www.us.army.smil.mil/suite/page/10531.

[5]"CIEDETS Lexicon," June 6, 2008. http://10.0.1.50/mediawiki/index.php/(U)_Terminal_Phase_of_IED_Deployment.

[6]Prominent examples of this situation can be found in the predeployment evaluations of the Highlighter and Night Eagle change detection systems conducted by ATEC and the evaluations of the Constant Hawk and Angel Fire persistent surveillance systems conducted by ATEC and the Marine Corps Systems Command, respectively.

References

Baker, R. G. and D. V. D'Aria. 2005. Countering IEDs and explosive hazards. *Engineer* 35: 32–35.

Gómez, M., A. Preece, M. Johnson, G. de Mel, W. Vasconcelos, C. Gibson, and A. Bar-Noy, et al. 2008. An ontology-centric approach to sensor-mission assignment. In *Proceedings of the 16th International Conference on Knowledge Engineering*: Practice and Patterns, September 29–October 2, 2008, Acitrezza, Italy. Goeloel, R., J. Siekmann, and W. Wablster (eds). Pages 347–363, Berlin/Heidelberg: Springer.

Goodwin, C., and D. J. Russomanno. 2006. An ontology-based sensor network prototype environment. In *Fifth International Conference on Information Processing in Sensor Networks*, April 19–21, Nashville, TN, pages 1–2. (Work in progress) Abstract available at http://ipsn.acm.org/2006/WIP/goodwin_1568983444.pdf.

Preece, A., M. Gomez, G. de Mel, W. Vasconcelos, D. Sleeman, S. Colley, and T. La Porta. 2008. Matching sensors to missions using a knowledge-based approach. In *SPIE Defense Transformation and Net-Centric Systems*, Orlando, FL: SPIE.

Russomanno, D. J., C. Kothari, and O. Thomas. 2005. Building a sensor ontology: A practical approach leveraging ISO and OGC models. In *The 2005 International Conference on Artificial Intelligence*, June 27–30, Las Vegas, NV, Arabnia, H. and R. Joshua (eds), 637–643. Las Vegas.

Russomanno, D. J., C. Kothari, and O. Thomas. 2005. Sensor ontologies: From shallow to deep models. In *Proceedings of the 37th Southeastern Symposium on Systems Theory*, March 20–22, Tuskegee, AL, 107–112. Piscataway, NJ: IEEE.

Simmons, B. M. and C. M. Wilcox. 2007. The four-element framework: a mission-focused test and evaluation strategy. *The ITEA Journal of Test and Evaluation* 28 (3): 61–66.

Thomas, O., and D. J. Russomanno. 2005. Applying the semantic web expert system shell to sensor fusion using dempster-shafer theory. In *Proceedings of the 37th Southeastern Symposium on Systems Theory*, March 20–22, Tuskegee, AL, 11–14. Piscataway, NJ: IEEE.